ZyWALL 2 Plus

Internet Security Appliance

Integrated with Complete Security Solutions Designed for Remote Office and SOHO

- ZyNOS ICSA IPSec VPN and FIREWALL Certified
- Web-based Content Filtering with Blue Coat service
- Policy-based Bandwidth Management
- Dial Backup with RS-232 on RJ-45 Null Modem Port
- Four LAN/ DMZ*10/100 auto MDI/MDIX Ethernet Ports
- 24Mbps throughput handing With Firewall On and Active VPN tunnel for FTTH and ADSL 2+

Benefits

Virtual Private Network (VPN) Connection
ZyWALL 2 Plus supports IPSec VPN suitable for remote site to central server deployment and home to office or office to home deployments. Data encryption over the Internet ensures secure transmission between the two sites eliminating the need for expensive leased lines, and enabling global interconnectivity at a minimal expense.
With the Redundant IPSec VPN feature, the ZyWALL 2 Plus can establish back-up tunnels to main sites.

Secured Firewall Protection and Blue Coat
The ZyNOS ICSA Firewall certified ZyWALL 2 Plus provides robust firewall protection, based on Stateful Packet Inspection (SPI) and Denial of Service (DoS) technology. The ZyWALL 2 Plus provides the first line of defense against hackers, and other malicious threats. BlueCoat subscription services assist in keeping spyware, malware and phishing exploits from attacking your PCs, and help protect business and family from illegal and unwanted surfing.

Maximum Bandwidth Provision
ZyWALL 2 Plus maximizes bandwidth utilization based on IP addresses and/or application types. Designed to ensure critical applications, services and specified users have the right amount of bandwidth when required.

Traffic Redirection for Broadband Backup Connection
ZyWALL 2 Plus increases reliability by supporting Fail-Over and Fail-Back technologies. User Selected back-up ISDN or Analog modem connections automatically switch traffic back to the WAN Port, when the primary connection is re-established. The ZyWALL 2 Plus backup feature ensures access to the net while decreasing the likelihood of potential down times and association losses.

Secure Zones Technology*
With the enhanced *DMZ zone, SOHO can easily deploy their access server or WIFI appliance separate from the trusted local network (LAN). The *DMZ zone has its own DHCP service and all zones are securely separated by firewall rules.

Specification

Mode of Operation

- Routing Mode
- Transparent Mode (Bridge)
- NAT (Network Address Translation)
- Dial Backup

Virtual Private Network

- 2 (5)* simultaneous IPSec VPN Connections
- DES/3DES/AES encryption
- Manual Key, IKE and PKI(X.509)
- IPSec NAT Traversal
- Xauth User Authentication
- Redundant VPN connection (VPN HA)

Firewall Security

- Transparent Firewall (Bridge mode)
- Stateful Packet Inspection
- DoS and DDoS Protection
- Real-time Attack Alert and Logs

Content Filtering

- Java/ActiveX/Cookie/ Proxy Blocking
- URL and Key word Blocking
- Web Content Filtering

Network

- DHCP client/server/relay
- PPPoE
- PPTP

System Management

- Web GUI (HTTP, HTTPS)
- Command Line Interface (Console, Telnet, SSH)
- Firmware Upgrade (Web GUI, TFTP/FTP/SFTP)
- Vantage Centralized Network Management*

Hardware Specifications

- Status LED Indicator : PWR, ACT, LAN 1~4, WAN
- Power adapter: 12VDC
- Console : RS-232 on RJ-45 Port
- Dial Backup : RS-232 on RJ-45 Null Modem Port
- Reset Button: Yes
- LAN/ DMZ*: 4-port switch, 10/100Mbps Auto MDI/MDIX
- WAN: 10/100Mbps Auto MDI/MDIX

Physical Specifications

- Dimensions: 181(W) x 128(D) x 36(H) mm
- Weight : 304g

<u>Environmental Specifications</u>

- Operating Temperature: 0°C ~ 50°C
- Operating Humidity: 20% ~ 95% (non-condensing)

<u>Certification</u>

- EMC: FCC Part 15 Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B
- Safety: CSA International, CE EN60950-1 (UL60950-1, CSA60950-1, EN60950-1, IEC60950-1)
- Green Product and WEEE comply with

* Firmware upgradeable for future

Note: DES/3DES/AES are not available in Russia